Blaine J. Benard (#5661)
Brent E. Johnson (#7558)
Engels J. Tejeda (#11427)
Emily T. Howe (#18294)
HOLLAND & HART LLP
222 South Main Street, Suite 2200
Salt Lake City, UT 84101-2194
Telephone: 801.799.5800
bjbenard@hollandhart.com
bjohnson@hollandhart.com
ejtejeda@hollandhart.com
ethowe@hollandhart.com

Attorneys for Defendant Uintah Basin Healthcare

**IN THE UNITED STATES DISTRICT COURT,
IN AND FOR THE DISTRICT OF UTAH, CENTRAL DIVISION**

JASON RASMUSSEN et al., on behalf of themselves and all others similarly situated, Plaintiffs, vs. UINTAH BASIN HEALTHCARE, a Utah non-profit corporation, Defendant.	**DEFENDANT'S MOTION TO DISMISS PLAINTIFFS' COMPLAINT UNDER FEDERAL RULES OF CIVIL PROCEDURE 12(b)(1) AND 12(b)(6), OR IN THE ALTERNATIVE, SUMMARY JUDGMENT UNDER RULE 56** Case No. 2:23-cv-00322-HCN-DBP District Judge Howard C. Nielson, Jr. Chief Magistrate Judge Dustin B. Pead

TABLE OF CONTENTS

Page No(s).

TABLE OF AUTHORITIES

Page No(s).

Cases

Statutes

Other Authorities

Defendant Uintah Basin Healthcare ("UBH") moves to dismiss this consolidated purported class action filed by Plaintiffs Jason Rasmussen, Mindy Rasmussen, Donna Halton, Doris Hyatt, Mandy Keasler, on behalf of her minor son A.K., and Christian Miller, on behalf of themselves and all others similarly situated (collectively, "Plaintiffs") pursuant to Fed. R. Civ. P. 12(b)(1) for lack of subject matter jurisdiction and pursuant to Fed. R. Civ. P. 12(b)(6) for failure to state a claim. Alternatively, Defendant moves for summary judgment because at the time of the data breach alleged in Plaintiffs' Complaint, Defendant was reasonably complying with a written cybersecurity program under the Utah Cybersecurity Affirmative Defense Act ("CADA"), Utah Code Ann. § 78B-4-702 *et seq*.

INTRODUCTION

UBH is an independent, rural healthcare system located in Duchesne County, Utah. Plaintiffs filed this purported class action seeking to capitalize on a cybersecurity attack that locked up some of UBH's computer systems and held data hostage until a ransom was paid (the "Incident"). The Incident may have involved personally identifiable information ("PII") and protected health information ("PHI"), but UBH promptly and aggressively responded to the Incident. To date, there is no evidence suggesting misuse or attempted misuse of the data implicated in the Incident.

As Plaintiffs allege, American businesses today face an onslaught of criminal cyberattacks designed to illicit ransom payments. As one U.S. District Court Judge summarized, "[t]here are only two types of companies left in the United States, according to data security experts: those that have been hacked and those that don't know they've been hacked." *Storm v Paytime, Inc*., 90 F. Supp 3d 359, 360 (M.D. Pa. 2015) (internal quotation marks omitted). Even

the United States Government has been the victim of multiple and significant cyberattacks where PII of millions of people has been compromised. To align with this reality, multiple courts have held that the mere occurrence of a data security incident does not give rise to a cause of action. Even more, recognizing the low likelihood of actual injury and that even the best prophylactic measure cannot protect businesses or individuals from insidious cybercriminals, the Utah legislature adopted CADA in 2021, effectively exculpating victims of data breaches from all liability where, as here, they reasonably complied with a written cybersecurity program under at least one of several recognized frameworks.

As shown below, courts in this circuit and elsewhere have repeatedly held that Plaintiffs' alleged damages do not sufficiently allege an actionable injury and have rightly dismissed class actions like this one for lack of subject matter jurisdiction under Rule 12(b)(1). Even if Plaintiffs had standing, diversity jurisdiction is lacking because the purported class fails to meet the requirements of the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA") since more than two thirds of the prospective class are citizens of Utah.

Alternatively, several of Plaintiffs' causes of action fail for failure to state a claim under Rule 12(b)(6), and UBH is entitled to summary judgment as to all of Plaintiffs' claims because the undisputed facts show that UBH was reasonably complying with a written security program qualified under CADA.

BACKGROUND

UBH is a healthcare system based in Roosevelt, Utah. Compl. ¶ 2. On or around November 7, 2022, UBH detected unusual activity on its network. *Id.* ¶ 4, *see also* Notice letter

attached here as Exhibit 1.[1] In response, UBH immediately secured the environment and engaged a leading cybersecurity firm to assist with an investigation and determine whether sensitive, personal, or protected health information may have been affected. *See* **Ex. 1** to the Declaration of Preston Marx in Support of this Motion ("**Marx Dec.**"), filed concurrently. On or around April 7, 2023, UBH determined the personal and protected health information of approximately 103,974 patients that received care with UBH between March 2012 and November 2022 may have been accessed or acquired without authorization during the Incident. *Id.*; Compl. ¶¶ 6, 35.

UBH then diligently worked to identify the names and addresses of individuals potentially impacted to provide notice. Ex. 1 at 1. On or about May 10, 2023, despite no evidence of misuse or attempted misuse of personal or protected health information, UBH notified the individuals whose information may have been compromised out of an abundance of caution. *Id.*; *see also* Compl. ¶ 3. The potentially affected information varied between individuals, but may have included names, dates of birth, addresses, Social Security numbers, health insurance information, and certain clinical details. Ex. 1 at 1; Compl. ¶ 1.

UBH informed the individuals of additional steps they could take to protect their information. Ex. 1 at 1-2. As an additional precaution, UBH offered all potentially impacted individuals, including Plaintiffs, identity theft protection services free of charge. *Id.* at 1. This included one year of credit and CyberScan monitoring, an identity theft insurance reimbursement policy, a fully managed identify recovery services, and assistance resolving any issues if an

[1] Plaintiffs discuss the notice that UBH sent to patients but fail to attach it to the Complaint. The Court may properly consider the notice on a motion to dismiss. *See Alvarado v. KOB-TV*, L.L.C., 493 F.3d 1210, 1215 (10th Cir. 2007) (noting a "district court may consider documents referred to in the complaint if the documents are central to the plaintiff's claim and the parties do not dispute the documents' authenticity").

affected person's identity becomes compromised. *Id.* Despite claiming to highly value privacy, Plaintiffs describe these security steps as "time-consuming" and complain the free, year-long data security program offered by UBH required them to "affirmatively sign up." Compl. ¶ 38. Only three of the named Plaintiffs took advantage of these protections offered by UBH. Compl. ¶ 126 (Hyatt), ¶ 165 (Jason Rasmussen), ¶ 177 (Mindy Rasmussen).

Plaintiffs, all of whom are citizens of Utah, have not incurred any concrete injury because of the Incident. Compl. ¶¶ 9, 14-19. Instead, most of Plaintiffs' Complaint is dedicated to *potential, future* damages that *could* arise from a data breach, but is devoid of any suggestion, let alone well pleaded facts, that Plaintiffs actually incurred any such damage. The remaining damages are wholly speculative or self-inflicted damages that lack any correlation to the Incident. As explained below, none of these damages establish standing.

STATEMENT OF UNDISPUTED FACTS IN SUPPORT OF SUMMARY JUDGMENT

1. UBH is an independent, rural 49-bed hospital that serves primarily local patients who live in Duchesne, Uintah, and Daggett Counties, Utah. *See* Marx Dec. ¶¶ 4-15.

2. UBH employs approximately 900 individuals, some of whom have access to patients' PII and PHI on an as needed basis. Marx Dec. ¶ 5.

3. On November 7, 2022, UBH detected the Incident. *See* Marx Dec. ¶ 16.

4. Prior to the Incident, UBH had adopted a written information security program (the "**WISP**") that included over a dozen policies and protocols regarding information security, including the following:

   a. ITS Security Policy 1.4; *see* Marx Dec. ¶ 17(a), **Ex. 2**;

   b. ITS Network Management Policy 2.2; *see* Marx Dec. ¶ 17(b), **Ex. 3**;

c. ITS Acceptable Use Policy 3.1; *see* Marx Dec. ¶ 17(c), **Ex. 4**;

d. ITS Employee Account Policy 4.2; *see* Marx Dec. ¶ 17(d), **Ex. 5**;

e. ITS Remote Access Policy 5.0; *see* Marx Dec. ¶ 17(e), **Ex. 6**;

f. ITS Business Continuity Policy 7.1; *see* Marx Dec. ¶ 17(f), **Ex. 7**;

g. ITS Asset Inventory Policy 8.0; *see* Marx Dec. ¶ 17(g), **Ex. 8**;

h. ITS Incident Response Policy 9.0; *see* Marx Dec. ¶ 17(h), **Ex. 9**;

i. ENG Physical Facilities Access Policy; *see* Marx Dec. ¶ 17(10), **Ex. 10**;

j. UBH Breach Notification Procedure; *see* Marx Dec. ¶ 17(j), **Ex. 11**.

5. As of the date of the Incident, Marx was serving as the Security Officer under the WISP. Marx Dec. ¶ 18.

6. As UBH's Security Officer, Marx oversaw implementation of and compliance with the WISP. Marx Dec. ¶ 19.

7. As of the date of the Incident, UBH was in substantial compliance with the WISP's policies and protocols. *See* Marx Dec. ¶¶ 20-31.

8. Consistent with the WISP's requirements, UBH engaged Inraprise Health – an outside, independent certified consultant – to conduct annual assessments of UBH's WISP from 2015 to 2022. *See* Marx Dec. ¶ 21.

9. A true copy of Intraprise's 2021 assessment of UBH's WISP, redacted to protect highly sensitive cybersecurity information, is attached as **Ex. 12** to Marx's Declaration. See Marx. Dec. ¶ 22.

10. A true copy of Intraprise's 2022 assessment of UBH's WISP, redacted to protect highly sensitive cybersecurity information, is attached as **Ex. 13** to Marx's Declaration. *See* Marx Dec. ¶ 23.

11. Intraprise attested that as between 2021 and 2022, including over the date of the Incident, UBH's WISP complied with the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), 45 C.F.R. Part 164 Subpart C and the applicable provisions of NIST Special Publication 800-53 and 800-53a. Marx Dec. ¶¶ 24-25; *see also*, **Ex. 14**.

12. Periodically, and at all times relevant to this lawsuit, UBH has taken steps to amend its policies and protocols to comply with recommendations made in the Intraprise assessments and to keep up with cybersecurity developments including regular updates to software security technology and recommended patches provided by UBH's software vendors. Marx Dec. ¶¶ 26-28. In addition, through UBH's contract with the Utah Education and Telehealth Network, weekly system vulnerability scans were conducted on UBH's circuits and edge equipment prior to and after the Incident. *Id.*

13. Consistent with the WISP, prior to and after the Incident, UBH adopted several risk mitigation protocols and processes, including standardizing operating systems for workstations, conducting monthly cybersecurity training for the information technology staff and quarterly anti-phishing testing and training for all staff, and deploying new technologies like network segmentation and monitoring software was they became available. *Id.*

14. As of the date of the Incident, the WISP was of an appropriate scope and scale based on the type of data that UBH handles, its size, and resources. *See* Declaration of Bruce Hartley in Support of this Motion ("**Hartley Dec.**") ¶¶ 16-21.

15. Among other things, UBH's engagement of third parties like Intraprise, its use of vulnerability scans by third parties like UETN, the frequency of those scans, its training schedules and policies are consistent with the best practices for similarly sized organizations that deal with similar data. *See id.*

16. Consistent with the WISP, on November 7, 2022, UBH retained an outside forensic consultant to help UBH contain, investigate and respond to the Incident. Marx Dec. ¶ 29.

17. On November 7, 2022, the outside consultant engaged with the threat actor on behalf of UBH. Marx Dec. ¶ 30.

18. On November 9, 2022, UBH confirmed the viability of its data backups and initiated restoration and recovery of the same. Marx Dec. ¶ 31.

19. On November 16, 2022, UBH reported the Incident to the Federal Bureau of Investigation. Marx Dec. ¶ 32.

20. On December 13, 2022, the threat actor provided UBH's consultant a decryption tool and represented it would restore all information potentially affected by the Incident. Marx Dec. ¶ 33.

21. On or around April 7, 2023, UBH determined the personal and protected health information of patients that received care with UBH between March 2020 and November 2022 may have been accessed or acquired without authorization during the Incident. Marx Dec. ¶ 34.

22. Although there is no evidence that the threat actor misused or published any data as a result of the Incident, UBH decided to notify all patients who received care between March 2012 and November 2022 about the Incident. Marx Dec. ¶ 35.

23. UBH hired a third party, Identity Theft Guard Solutions, Inc., d/b/a IDX to notify the patients. IDX submitted all names and addresses to the National Change of Address databank to secure current addresses. IDX confirmed that 91,950 of the 103,974 individuals who received care between March 2012 and November 2022 had Utah addresses. Marx Dec. ¶ 36.

24. On May 10, 223, UBH notified the potentially affected individuals of the Incident. Marx Dec. ¶¶ 37-38; *see e.g.*, Ex. 1.

25. UBH does not retain patient payment card data on its system and none of its investigations has revelated that payment card data was exposed or potentially exposed during the Incident. Marx Dec. ¶ 39.

ARGUMENT

I. LEGAL STANDARDS

Defendants seek dismissal on three alternative grounds: lack of subject matter jurisdiction under Rule 12(b)(1), failure to state a claim upon which relief can be granted under Rule 12(b)(6), or summary judgment under Utah's CADA and Rule 56.

A motion to dismiss for lack of subject matter jurisdiction brought under Rule 12(b)(1) takes two forms: either a "facial" or a "factual attack." *Stuart v. Colorado Interstate Gas Co.*, 271 F.3d 1221, 1225 (10th Cir. 2001).[2] A facial attack challenges the sufficiency of the complaint's allegations, which are accepted as true, as to the existence of subject matter

[2] Subject matter jurisdiction is a "constitutional prerequisite to hearing a case." *Gad v. Kan. State Univ.*, 787 F.3d 1032, 1035 (10th Cir. 2015). The burden to establish subject matter jurisdiction rests with the Plaintiffs. *Southway v. Cent. Bank of Nig.*, 328 F.3d 1267, 1274 (10th Cir. 2003). A party may move to dismiss a complaint for lack of subject matter jurisdiction, including dismissal for lack of standing, under Rule 12(b)(1). Fed. R. Civ. P. 12(b)(1); *see Hill v. Vanderbilt Cap. Advisors, LLC*, 702 F.3d 1220, 1222, 1224 (10th Cir. 2012).

jurisdiction. *Id.* By contrast, in a factual attack, "a party may go beyond allegations contained in the complaint and challenge the facts upon which subject matter jurisdiction is based." *Id.* A court may not presume the truthfulness of the complaint's allegations when analyzing a factual attack. *McCollin v. United States Army Corps of Eng'rs*, No. 2:12-cv-1022 TS, 2013 U.S. Dist. LEXIS 175432, at *5 (D. Utah Dec. 11, 2013). And the court has "wide discretion to allow affidavits, other documents, and a limited evidentiary hearing to resolve disputed jurisdictional facts," without turning the motion into a motion for summary judgment. *Stuart*, 271 F.3d at 1225 (internal quotation marks omitted). Thus, in opposing a factual attack on subject matter jurisdiction, the plaintiffs "must [] present evidence necessary to satisfy [their] burden of establishing that the court possesses subject matter jurisdiction." *McCollin*, 2013 U.S. Dist. LEXIS 175432, at *5. When Plaintiffs seek to represent a class, they must allege "they personally have been injured, not that injury has been suffered by other, unidentified members of the class." *Warth v. Seldin*, 422 U.S. 490, 502 (1975). Here, as shown below, the Complaint's jurisdictional allegations are both facially and factually deficient.

Separately, a complaint fails under Rule 12(b)(6) if the alleged facts do not entitle the plaintiff to relief. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 560-61 (2007). To survive a motion to dismiss, a plaintiff is required to do more than recite "labels and conclusions[,] . . . a formulaic recitation of the elements of a cause of action will not do." *Id.* at 555. Legal conclusions "must be supported by factual allegations." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009).

Lastly, in the Tenth Circuit, a defendant may use a motion for summary judgment to assert an affirmative defense that entitles it to judgment as a matter of law. *Helm v. Kansas*, 656

F.3d 1277, 1284 (10th Cir. 2011); *see also*, Fed. R. Civ. P. 56(a).[3] In such instances, once the movant meets its initial burden to "demonstrate that no disputed material fact exists regarding the affirmative defense asserted . . . the plaintiff must then demonstrate with specificity the existence of a disputed material fact." *Helm*, 656 F.3d at 1284 (internal quotation marks omitted). If the plaintiff fails to do so, "the affirmative defense bars [the] claim, and the defendant is then entitled to summary judgment as a matter of law." *Id.* (internal quotation marks omitted)."A fact is 'material' if, under the governing law, it could have an effect on the outcome of the lawsuit." *Jones v. Norton*, 809 F.3d 564, 573 (10th Cir. 2015) (internal citation omitted). "A dispute over a material fact is 'genuine' if a rational jury could find in favor of the nonmoving party on the evidence presented." *Id.*

Here, Plaintiffs' Complaint is subject to dismissal under Rule 12(b)(1) because it fails to establish subject matter jurisdiction on its face and lacks properly plead facts supporting CAFA jurisdiction, the Complaint fails to state a claim under which relief can be granted under Rule 12(b)(6), and Defendant is entitled to summary judgment under Utah's CADA.

II. DISMISSAL IS WARRANTED UNDER RULE 12(b)(1) BECAUSE ON ITS FACE, PLAINTIFFS' COMPLAINT FAILS TO ESTABLISH ARTICLE III STANDING.

To establish federal subject matter jurisdiction, "the plaintiff[s] [have] the burden of establishing each of [the] three elements of Article III standing." *Nova Health Sys. v. Gandy*, 416 F.3d 1149, 1154 (10th Cir. 2005). That is, Plaintiffs must show they "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to

[3] Where, as here, neither the local rules nor the Court have ordered otherwise, "a party may file a motion for summary judgment at any time until 30 days after the close of all discovery." Fed. R. Civ. P. 56(b).

be redressed by a favorable judicial decision." *Lupia v. Medicredit, Inc*., 8 F.4th 1184, 1190 (10th Cir. 2021) (internal quotation marks omitted). Individual standing is a threshold for all actions, including class actions. *Big Elk v. Bd. of Cty. Comm'rs,* 3 F. App'x 802, 807 (10th Cir. 2001). Moreover, "[s]tanding is determined as of the time the action is brought." *Nova Health Sys.*, 416 F.3d at 1154.

A. Plaintiffs Do Not Have Standing Because They Have Not Alleged Any Injury In Fact.

To constitute an injury in fact, the injury must be "an invasion of a legally protected interest," that is "concrete and particularized and actual or imminent," not one that is "conjectural or hypothetical." *Lupia*, 8 F.4th at 1190 (internal quotation marks omitted). That is, the injury must be "real" instead of "abstract." *Id.* Simply put, "[n]o concrete harm, no standing." *Id.* (internal quotation marks omitted). If a plaintiff seeks to base standing on a "threatened injury[,]" it "must be *certainly impending* to constitute injury in fact." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (emphasis in original) (internal quotation marks omitted). Beyond this, the injury "has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court." *N.M. ex rel. State Eng'r v. Carson*, 908 F.3d 659, 665 (10th Cir. 2018) (internal quotation marks omitted). Consequently, evidence of a data breach alone does not satisfy standing requirements. *See O'Leary v. Trustedid, Inc*., 60 F.4th 240, 244 (4th Cir. 2023) ("[B]eing subject to a data breach isn't in and of itself sufficient to establish Article III standing.").

Here, the named Plaintiffs allege seven categories of purported injuries: (1) mitigation efforts; (2) unauthorized charges; (3) suffering from fear, anxiety, annoyance, inconvenience, and nuisance; (4) loss of privacy and diminution in value of private information; (5) loss of the

benefit of the bargain; (6) increase in spam; and (7) future damages. None of these theories establish standing.

1. Mitigation Costs.

Each Plaintiff claims to have spent between one and fifteen hours researching the Incident and undertaking mitigation efforts such as changing passwords and updating accounts.[4] Relatedly, Plaintiff Halton claims she spent a nominal amount on gas driving to and from her bank, Compl. ¶ 114, and Plaintiff Mindy Rasmussen purchased identity theft and password protection at the cost of $18 per month, *id.* ¶ 178.

As a matter of law, Plaintiffs' mitigation efforts and related costs fail to constitute an injury in fact to satisfy standing. The Supreme Court rejected this same theory of damages. *See Clapper*, 568 U.S. at 416. The *Clapper* Court held plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.* If the law allowed otherwise, "an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." *Id.*

Following *Clapper*, courts almost uniformly reject mitigation costs as constituting a sufficient "injury in fact" to establish standing in data breach cases. *See, e.g., McCombs v. Delta Grp. Elecs., Inc.,* No. 1:22-cv-00662, 2023 U.S. Dist. LEXIS 100632, at *15-16 (D.N.M. June 9, 2023) (plaintiff's "manufactured harm" incurred in response to speculative future harm did not give rise to standing); *Blood v. Labette Cnty. Med. Ctr*., No. 22-04036, 2022 U.S. Dist. LEXIS

[4] Compl. ¶ 113 (Halton); ¶ 126 (Hyatt); ¶ 139 (Keasler); ¶ 151 (Miller); ¶ 165 (Jason Rasmussen); ¶ 177 (Mindy Rasmussen).

191922, at *7, 14-15 (D. Kan. Oct. 20, 2022) (concluding that "[n]one of the named plaintiffs adequately alleges standing to pursue the claims" and despite alleging time spent monitoring and mitigating).

Accordingly, Plaintiffs' mitigation efforts are not an injury in fact and fail to establish standing.

2. Unauthorized Charges.

Plaintiff Halton claims she received two unauthorized charges on her debit card but does not allege that she was held financially responsible for those charges. Compl. ¶ 114. Plaintiff Miller claims he had a single unauthorized charge, in an amount less than $10, from his checking account, but the charge failed to process. *Id.* ¶ 152. No other Plaintiff alleges any unauthorized charges and not a single Plaintiff alleges any improper charges for which they were held financially responsible.

Even where actual fraudulent credit card charges are made after a data breach, if the plaintiff is not held financially responsible for paying for such charges, the injury requirement is not satisfied. *Green v. eBay Inc*., No. 14-1688, 2015 U.S. Dist. LEXIS 58047, at *13-14 (E.D. La. May 4, 2015). Where Plaintiffs Halton and Miller claim they received unauthorized charges but fail to allege that they were held financially responsible for those charges or incurred any future expenses because of those charges, this damage theory fails to satisfy standing.

3. Fear, Anxiety, Annoyance, Inconvenience, and Nuisance.

All Plaintiffs, except for A.K.,[5] allege that as a result of the Incident they suffer from "fear, anxiety, annoyance, inconvenience, and nuisance."[6] These bare claims of emotional injuries, without any supporting facts, do not constitute an injury in fact. *Beck v. McDonald*, 848 F.3d 262, 272 (4th Cir. 2017) (rejecting claim that "emotional upset and fear [of] identity theft and financial fraud resulting from the data breaches" are sufficient to confer Article III standing); *see also Stamat v. Grandizio Wilkins Little & Matthews, LLP*, No. SAG-22-00747, 2022 U.S. Dist. LEXIS 158224, at *19-20 (D. Md. Aug. 31, 2022) (bare assertions of emotional injury do not satisfy Article III standing).

The totality of the Plaintiffs' allegations that they suffer from these emotional ailments is a single conclusory sentence without any factual support. These bare bones assertions are not injuries in fact and fail to establish standing.

4. Loss of Privacy and Diminution in Value of Private Information.

Plaintiffs allege broad and conclusory damages in terms of loss and invasion of privacy and "diminution in value of private information."[7] And Plaintiff Hyatt claims her personal

---

[5] Keasler alleges that she suffers these ailments due to the data breach, not Plaintiff A.K. Compl. ¶ 143. The Court should disregard damages Keasler asserts she suffered personally, as opposed to those damages suffered by A.K. (on behalf of whom the case is brought). *See Holly Sugar Corp. v. Goshen Cty. Coop. Beet Growers Asso.,* 725 F.2d 564, 570 (10th Cir. 1984) ("A plaintiff's claim for relief absent a statutory provision or judicially created exception cannot be based on allegations of injury to third parties.").

[6] Compl. ¶ 118 (Halton); ¶ 131 (Hyatt); ¶ 157 (Miller); ¶ 169 (Jason Rasmussen); ¶ 183 (Mindy Rasmussen).

[7] Compl. ¶¶ 115, 119 (Halton); ¶¶ 128, 132 (Hyatt); ¶¶ 140, 144 (Keasler on behalf of A.K.); ¶¶ 154, 158 (Miller); ¶¶ 166, 170 (Jason Rasmussen); ¶¶ 180, 184 (Mindy Rasmussen).

information has been disseminated on the dark web.[8] *Id.* ¶ 127. Courts have repeatedly found that mere allegations of loss of privacy and diminution in value of private information do not constitute actionable injuries.

First, Plaintiffs do not allege any facts to support a suggestion that their data had a specific monetary value. Nor could they, as courts "routinely reject[] the proposition that an individual's personal identifying information has an independent monetary value." *Welborn v. IRS*, 218 F. Supp. 3d 64, 78 (D.D.C. 2016).

And in any event, this Court need not determine if the private information has monetary value, because even if it did, Plaintiffs do not establish the Incident resulted in a reduction of its alleged value. *See id.* (finding no injury in fact where plaintiffs did not allege facts to support inference that their personal information became less valuable). Rejecting the same argument, the court in *Stamat* ruled the plaintiff failed to satisfy standing by making general claims of diminution of value in PII. *Stamat v. Grandizio Wilkins Little & Matthews, LLP*, No. SAG-22-00747, 2022 U.S. Dist. LEXIS 158224, at *18 (D. Md. Aug. 31, 2022). Rather than present evidence as to how the alleged value of his PII had been lowered, the plaintiff presented research on how much others would likely pay for his stolen information. *Id.* at *18-19. The court rejected this supporting evidence, finding "[t]he fact that someone else can profit from having access to his information does not necessarily lower the value of that information to [plaintiff]." *Id.* at *19.

[8] Plaintiff Hyatt does not allege any factual support for this allegation. She does not allege how it was determined that her personal information was disseminated on the Dark Web nor does she state what personal information she believes was disseminated. It is possible to conduct a search of the Dark Web to see what, if any, personal information is disseminated as well as attempt to link any dissemination with a particular breach.

Plaintiffs would need to establish more to prove damage based on diminution in value. For example, Plaintiffs would need to establish they attempted to sell their personal information and that because of the data breach, they were forced to accept a decreased price. *Chambliss v. CareFirst, Inc*., 189 F. Supp. 3d 564, 572 (D. Md. 2016); *see also Legg v. Leaders Life Ins. Co*., 574 F. Supp. 3d 985, 994 (W.D. Okla. 2021) (finding no standing where plaintiff "fails to allege that he attempted to sell his personal information and was forced to accept a decreased price.").

Here, like the above cases, Plaintiffs cannot show that the Incident resulted in a decrease in the value of their private information. No Plaintiff established their private information had monetary value. And not a single Plaintiff alleged they sought to sell the private information and was unable to fetch the desired price as a result of the Incident. Thus, this theory of damages does not constitute an injury in fact and does not establish standing.

5. Loss of the Benefit of the Bargain.

Several of the Plaintiffs allege they lost "the benefit of the bargain [they] made with [UBH] by overpaying for services that were intended to be accompanied by adequate data security but were not."[9] This theory of injury is "consistently rejected in data breach cases where plaintiffs have not alleged that the value of the goods or services they purchased was diminished as a result of the data breach." *Chambliss*, 189 F. Supp. 3d at 572.

Here, Plaintiffs only make conclusory allegations that they lost the benefit of the bargain. First, Plaintiffs do not specify what they actually paid for services by UBH. Nor do Plaintiffs allege any specific facts to suggest any price they did pay incorporated some form of protection

[9] Compl. ¶ 121 (Halton); ¶ 146 (Plaintiff Keasler on behalf of A.K.); ¶ 172 (Jason Rasmussen); ¶ 186 (Mindy Rasmussen). Plaintiff Hyatt, does not allege that she overpaid for services, but only generally claims "loss of the benefit of the bargain." *Id*. ¶ 127.

premium for data security, or that both the Plaintiffs and UBH understood the premium was to be used for data security. Beyond this, Plaintiffs do not allege any facts to suggest the Incident diminished the value of the medical services they received from UBH. These general allegations fail to satisfy an injury in fact to establish standing.

6. Increase in Spam.

Plaintiffs Hyatt, Miller, and Mindy Rasmussen allege they received an increase in spam communications. Compl. ¶ 127 (Hyatt – spam calls, texts, and/or emails), ¶ 153 (Miller – spam calls, texts, and emails), ¶ 179 (Mindy. Rasmussen – spam calls). Plaintiffs' alleged inconvenient disruptions are common in today's digitized society and do not constitute an injury in fact. *See McCombs*, 2023 U.S. Dist. LEXIS 100632, at *18-19 (collecting cases finding unsolicited spam insufficient to constitute an injury in fact); *In re Practicefirst Data Breach Litig.,* No. 1:21-cv-00790, 2022 U.S. Dist. LEXIS 19272, at *18 n.8 (W.D.N.Y. Feb. 1, 2022) (same). Nor does an increase in spam suggest misuse of Plaintiffs' private information. *See Legg*, 574 F. Supp. 3d at 993 (finding that "the receipt of phishing emails . . . does not plausibly suggest that any actual misuse of [p]laintiff's personal identifying information has occurred).

Accordingly, Plaintiffs Hyatt, Miller, and Ms. Rasmussen's claims of increase in spam fail to establish an injury in fact.

7. Future Damages.

Unable to show any actual damages, Plaintiffs claim wildly speculative future damages: "substantial risk of imminent harm" for the rest of their lives; continued risk and harm to private

information; and anticipated additional time and money to mitigate and address present and impending injuries caused by the Incident.[10] These allegations fair no better.

The *Clapper* Court clarified, allegations of "*possible* future injury" or even an "objectively reasonable likelihood" of future injury are insufficient to confer standing. *Clapper*, 568 U.S. at 409-10 (emphasis in original). A future injury can only constitute an Article III injury-in-fact "if the threatened injury [is] *certainly impending*." *Id.* at 409 (emphasis in original). Theories that rely upon "highly attenuated chain of possibilities" do not satisfy this standard. *Id.* at 410; *see also McCombs*, 2023 U.S. Dist. LEXIS 100632, at *10 (District Courts within the Tenth Circuit "have followed the majority view concluding that a plaintiff does not suffer an injury in fact where their PII is accessed through a data breach but no direct harm results"); *Legg,* 574 F. Supp. 3d at 994 ("Plaintiff only pleads facts showing that there is a non-imminent risk of possible future injury following the data breach. This is not sufficient to confer standing").

The mere threat that such information could be improperly used is not sufficient to establish standing. *Green*, 2015 U.S. Dist. LEXIS 58047, at *19. In part because it is "well settled that a claim of injury generally is too conjectural or hypothetical to confer standing when the injury's existence depends on the decision of third parties." *Id.* at *17-18 (internal quotation marks omitted); *see also McCombs*, 2023 U.S. Dist. LEXIS 100632, at *13 (D.N.M. June 9, 2023) (noting future risk of improper use of PII "falls well short of what is required" to establish standing). One court emphasized that "courts cannot be in the business of prognosticating

[10] Compl. ¶¶ 116-17, 121 (Halton); ¶¶ 127, 129-130 (Hyatt); ¶¶ 141, 146 (A.K.), ¶ 142 (Keasler on behalf of A.K.); ¶¶ 155-56, 160 (Miller); ¶¶ 167-68, 172 (Jason Rasmussen); ¶¶ 181-82, 186 (Mindy Rasmussen).

whether a particular hacker was sophisticated or malicious enough to both be able to successfully read and manipulate the data and engage in identity theft." *Storm*, 90 F. Supp. 3d at 368. Until the hacker does misuse the personal information for personal gain, the plaintiff simply has no injury to establish standing. *Id.* Moreover, "as the breaches fade further into the past, the Plaintiffs' threatened injuries become more and more speculative." *Beck*, 848 F.3d at 275 (internal quotation marks omitted).

Here, Plaintiffs' alleged risks of potential future harm are not certainly impending. As in *Green*, "the existence of Plaintiff's alleged injury in this case rests on whether third parties decide to do anything with the information. If they choose to do nothing, there will never be an injury." *Green*, 2015 U.S. Dist. LEXIS 58047, at *16-17. The Complaint is devoid of specific facts to suggest any of the claimed future harms are "certainly impending." This is coupled with the fact that, despite that it has been almost a year since the Incident, Plaintiffs have not identified a single cognizable harm. Plaintiffs' future damages are speculative at best and are wholly contingent on the acts of third parties. And given the amount of time that has passed, any potential future harm is becoming even more speculative. Plaintiffs' future damages are too remote and speculative to constitute an injury in fact.

All of Plaintiffs' alleged theories of damages fail to satisfy the Article III standing requirement. Where the Complaint fails to establish one of the three required elements of standing, it should be dismissed.

B. Plaintiffs Lack Standing Because Their Injuries, If Any, Are Not Traceable To The Incident.

Even if this Court were to find any of Plaintiffs' damages theories sufficient to allege an injury in fact, the Plaintiffs still do not have standing because they have not met their burden to

establish that their injuries, if any, are traceable to the Incident. Traceability requires "a causal connection between the injury and the conduct complained of" -- that is the injury must be fairly traceable "to the challenged action of the defendant," not the result of an "independent action of some third party not before the court." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (internal quotation marks omitted). Here, none of Plaintiffs' alleged damages are traceable to the Incident.

First, on its face, the Complaint fails to properly plead that the fraudulent activity purportedly endured by Plaintiffs is linked to, let alone the result of, the Incident. For example, there is no factual support for the implied inference that the alleged unauthorized charges or increased spam emails relate to the Incident. For these allegations to even approach the detail requisite to plead standing, the Court would have to guess that the charges by unknown individuals (for which Plaintiffs were not financially liable) originated from the Incident. The Court would have to similarly guess as to the root cause of the alleged increase in spam because the Complaint is devoid of any related well pleaded facts, including, for example, the subject matter of the alleged calls or who made them.

The Tenth Circuit has made clear that "[t]raceability is absent when [the court has] to guess why the third parties acted as they did." *Northern Laramie Range Alliance v. Fed. Energy Regulatory Comm'n*, 733 F.3d 1030, 1035 (10th Cir. 2013). And the assumption would not be warranted in any event. As the court noted in *Storm*, a 2014 Ponemon Institute report noted 43% of companies experienced a data breach in the prior year. *Storm*, 90 F.Supp.3d at 360. So it is not a given, or even probable, that if Plaintiffs were in fact victims of a data breach, their purported injuries originated with the Incident. Nor are Plaintiffs' phone numbers and email addresses even

among the information that they allege was hacked. *See* Compl. ¶ 6. Plaintiffs' claims of future damages are even less related to the Incident. Plaintiffs suggest that damage and risk to their private information will last for the rest of their lives. *See* Compl. ¶¶ 116, 129, 141, 155, 167, 181. But it is nearly impossible to determine, and the Complaint has certainly not established, that any future potential improper use of private information is a result of this Incident and not another, unrelated data breach.

Second, Plaintiffs' injuries, if any, are not traceable to UBH because they were caused by a third-party. *See, e.g.*, *Peters v. St. Joseph Services Corp.*, 74 F.Supp.3d 847 (S.D. Texas 2015). In *Peters*, a data breach potentially compromised personal information, and the plaintiff alleged that unknown third parties attempted to use her credit card and sent her spam. *Id.* at 850-51. The plaintiff argued the injuries were traceable to defendant's security failures. *Id.* at 857. The court disagreed, finding, "[a]lthough it is alleged that [the defendant's] failures 'proximately caused' these injuries, the allegation is conclusory and fails to account for the sufficient break in causation caused by opportunistic third parties." *Id*. To the extent the alleged injuries satisfy injuries in fact, they are "'the result of the independent action of a third party' and therefore not cognizable under Article III." *Id.* (quoting *S. Christian Leadership Conference v. Supreme Court of State of La.*, 252 F.3d 781, 788 (5th Cir. 2001)).

Plaintiffs' allegation that their purported injuries are traceable to the Incident is conclusory. More importantly, like *Peters*, even if the damages alleged were somehow caused by the Incident, Plaintiffs cannot establish traceability because their injuries are the result of the independent action of a third party and therefore not cognizable under Article III. In sum, Plaintiffs simply cannot show that their alleged injuries – whether materialized or anticipated –

are traceable to UBH's conduct. Consequently, Plaintiffs fail to establish the required traceability element of standing and the Court should dismiss the case.

C. Plaintiffs Lack Standing Because They Have Not Established Their Injuries, If Any, Are Redressable.

Even if Plaintiffs had alleged an injury in fact, and even if that injury was traceable to UBH's conduct, they still lack standing because they have not met their burden to show that their injuries are "redressable by a favorable ruling." *Clapper*, 568 U.S. at 409. To satisfy this element of standing "it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Thompson v. Lengerich*, 798 F. App'x 204, 210 (10th Cir. 2019). Courts have found claims fail the redressability element where the plaintiff does not allege any quantifiable damage or loss suffered as a result of a data breach. *Peters*, 74 F. Supp. 3d at 857.

Here, there is no suggestion that Plaintiffs' alleged damages will be redressed by a favorable decision and any argument to the contrary is rank speculation. *See generally*, Prayer for Relief, Compl. at 68. Plaintiffs fail to establish how a favorable decision will remedy the harm from the alleged unauthorized charge, for which Plaintiffs were not financially responsible; or will stop the alleged increase in spam from third parties not before this Court; or remedy their loss of privacy and diminution in value of private information which does not have an inherent value and for which Plaintiffs have not identified any monetary loss. Along the same lines, Plaintiffs have not alleged that any favorable judgment will remedy the "loss of the benefit of the bargain" or remedy the speculative future damages. Plaintiffs fail to establish it is likely their harms will be redressed by a favorable decision.

III. DIMISSAL IS WARRANTED UNDER RULE 12(b)(1) BECAUSE PLAINTIFFS FAIL TO PLEAD SUFFICIENT FACTS TO ESTABLISH DIVERSITY JURISDICTION UNDER CAFA.

On a factual attack, the parties may go beyond the pleadings and a court cannot presume the truthfulness of the complaint's allegations. *Stuart*, 271 F.3d at 1225; *McCollin*, 2013 U.S. Dist. LEXIS 175432, at *5. Here, despite alleging only state law claims, Plaintiffs bring this action in Federal Court on the grounds of diversity jurisdiction. *See* Compl. ¶ 21. Plaintiffs, as the parties seeking to invoke the Court's jurisdiction, bear the burden of proof to establish diversity. *Hertz Corp. v. Friend*, 559 U.S. 77, 96-97 (2010).

Plaintiffs claim they meet diversity jurisdiction under CAFA, because they allege, among other things, many of the class members "have different citizenship from [UBH]." Compl. ¶ 21. Plaintiffs concede that UBH's principal place of business is in Utah. *Id.* ¶ 20. Thus, there is no dispute that UBH is a citizen of Utah. *See Grynberg v. Kinder Morgan Energy, Ltd. P'ship*, 805 F.3d 901, 905 (10th Cir. 2015) ("For diversity, a corporation is a citizen of its state of incorporation and the state where its principal place of business is located.").

However, under CAFA, a court "shall decline to exercise jurisdiction" when "two-thirds or more of the members of all proposed plaintiff classes in the aggregate, and the primary defendants, are citizens of the State in which the action was originally filed." 28 U.S.C. § 1332(d)(4)(B). Here, there is no dispute that UBH, the only defendant, is a citizen of Utah and that the action is originally filed in Utah. Thus, if at least two-thirds of the members of the proposed class are also citizens of Utah, this Court must decline to exercise jurisdiction.

When determining citizenship, "[a] person is a citizen of a state if the person is domiciled in that state" *Reece v. AES Corp.*, 638 F. App'x 755, 769 (10th Cir. 2016) (internal quotation

marks omitted). A person acquires domicile in a state "when the person resides there *and* intends to remain there indefinitely, which is established by the totality of the circumstances." *Id.* (emphasis in original) (internal quotation marks omitted). An individual's "place of residence is *prima facie* the domicile," but "allegations of mere residence may not be equated with citizenship." *Id.* (internal quotation marks omitted).

Plaintiffs do not present any satisfactory evidence to establish that at least one-third of the putative class members are citizens of states other than Utah. The proposed class is the 103,974 patients that received care with UBH between March 2012 and November 2022. Compl. ¶¶ 35, 192. All of the named Plaintiffs are citizens of Utah. Compl. ¶¶ 14-19. Plaintiffs only rely upon state lists of residents allegedly impacted by the Incident. Based on the documents cited by Plaintiffs: 16 Maine residents were impacted; 1120 Texas residents were impacted; 72 Massachusetts residents were impacted; 59 Indiana residents were impacted; no number is listed for Oregon residents; and the link for the Vermont notice does not work. *Id*. ¶ 21 n. 1. Although residency does not establish citizenship, even presuming that the 1,267 individuals identified were in fact citizens of other states, these individuals constitute just over one percent of the proposed class, nowhere near the required one-third.

In contrast, approximately 88 percent of the members of the proposed class are Utah citizens. When the Incident occurred, UBH reviewed its records to identify the addresses of all 103,974 individuals. Marx Dec. ¶ 36. Of the 103,974 individuals, 91,950 had Utah addresses. *Id.* UBH hired IDX, a leading data breach response provider, to send the Notice Letter to the putative class members. *Id.* Before mailing, IDX submitted all names and addresses to the National Change of Address databank to secure current addresses. *Id.* After updating addresses

for about 8,700 people, 91,950 individuals had Utah addresses. *See id.* The continuance of Utah addresses, both those that had not changed and those that had new addresses still located in Utah, evidence that these individuals are located in Utah with an intent to remain here – and thus are Utah citizens.

This fact is further strengthened by the very nature of UBH and Duchesne County. UBH is an independent rural healthcare system located in Duchesne County, Utah, a rural area in the northeast section of the state. Marx Dec. ¶ 4. As a 49-bed hospital facility along with local clinics, UBH largely serves local individuals—Utah citizens living in Duchesne, Uintah, and Daggett Counties or nearby. *Id.* ¶¶ 4-15. In 2020, 97.89% of UBH patients provided Utah addresses to UBH's registration department. *Id.* ¶ 8; *see also* Ex. 15. In 2021, 98.30% of UBH patients had Utah addresses; in 2022, 98.43% of UBH patients had Utah addresses; and through August of 2023, 98.57% of UBH patients have Utah addresses. *Id.* ¶¶ 9-11. Simply put, the patients served by UBH and therefore members of the putative class, are almost entirely citizens of Utah as opposed to individuals needing services while visiting second homes, passing through, or on vacation.

In short, Plaintiffs have not established that anywhere near one-third of the putative class members are citizens of states other than Utah. Well over two-thirds of the class are, in fact, citizens of Utah, which defeats diversity jurisdiction. Thus, the Complaint must be dismissed for lack of standing.

IV. IN THE ALTERNATIVE, CADA BARS THE COMPLAINT IN WHOLE BECAUSE UBH REASONABLY COMPLIED WITH A QUALIFIED WRITTEN SECURITY PROGRAM AS OF THE DATE OF THE INCIDENT.

Plaintiffs' claims fail because as of the date of the Incident, UBH had created, maintained and reasonably complied with a written information security program – or WISP – under CADA. *See* Utah Code Ann. § 78B-4-701 *et seq*.

CADA establishes an affirmative defense to any claim filed in Utah, or under Utah law, alleging that a victim of a cyberattack failed to prevent,[11] respond to,[12] or give adequate notice of,[13] a data breach where, as of the date of the incident, the victim "reasonably complie[d]" with a WISP that meets the threshold standards outlined in Section 702 of CADA. *See* Utah Code

---

[11] "A person that creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (4), and is in place at the time of the breach of systems security of the person, has an affirmative defense to a claim that: (a) is brought under the laws of this state or in the courts of this state; and, (b) alleges that the person failed to implement reasonable information security controls that resulted in the breach of system security." Utah Code Ann. §§ 78B-4-702(1)(a)-(b). UBH is a "person" within the meaning of CADA because that term includes an "association," "corporation," or "any unincorporated organization." Utah Code Ann. § 78B-4-701(4)(a)(ii), (iii), (iv).

[12] "A person has an affirmative defense to a claim that the person failed to appropriately respond to a breach of system security if: (a) the person creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (4) and is in place at the time of the breach of system security; and (b) the written cybersecurity program had protocols at the time of the breach of system security for responding to a breach of system security that reasonably complied with the written cybersecurity program under Subsection 2(a) and the person followed the protocols." Utah Code Ann. §§ 78B-4-702(2)(a)-(b).

[13] "A person has an affirmative defense to a claim that the person failed to appropriately notify an individual whose personal information was compromised in a breach of system if: (a) the person creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (4) and is in place at the time of the breach of system security; and (b) the written cybersecurity program had protocols at the time of the breach of security for notifying an individual about a breach of system security that reasonably complied with the requirements for a written cybersecurity program under Subsection (3)(a) and the person followed the protocols." Utah Code Ann. §§ 78B-4-702(3)(a)-(b).

Ann. §§ 78B-4-702(1)-(4). In a nutshell, the WISP must include protocols for responding to, and giving notice of, a breach; the victim must have complied with those protocols; and the WISP must reasonably conform to at least one of the alternative frameworks set out in subsection 702(4). *See id.* at §§ 78B-4-702(1)-(3).

Here, CADA governs all of Plaintiffs' claims because they arise under Utah law and are based on Plaintiffs' allegations that UBH purportedly failed to prevent, properly respond to, or timely notify them of, the Incident. *See Erie R. Co. v. Tompkins*, 304 U.S. 64 (1938) (federal courts sitting in diversity apply the substantive law of the state in which the case arose); *see also*, Compl. ¶¶ 5, 12, 71-72, 193(d), 251 (alleging UBH failed to prevent, properly respond, or timely notify Plaintiffs of the Incident). Moreover, UBH is entitled to summary judgment on its affirmative defense under CADA because UBH's WISP complied with the design, framework, and proportionality requirements of subsection 702(4). *See* Utah Code Ann. § 78B-4-702(4).

A. UBH's WISP Was Properly Designed Within The Meaning Of Utah Code Ann. § 78B-4-702(4)(a).

To qualify for the affirmative defense, the cybersecurity program must "provide administrative, technical, and physical safeguards" to protect personal information, including:

> being designed to:
>
> (i) protect the security, confidentiality, and integrity of personal information;
>
> (ii) protect against any anticipated threat or hazard to the security, confidentiality, or integrity of persona information; and,
>
> (iii) protect against a breach of system security.

Id. §§ 78B-4-702(4)(a)(i)-(iii).

UBH's WISP met all three of these criteria as of the date of the Incident. *See* Hartley Dec. ¶¶ 19-24. The WISP consisted of over a dozen policies and protocols outlining administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of PII and PHI. *See* Marx Dec. ¶ 17. For example, the WISP's ITS Security Policy 1.4 defined the standards and procedures governing the physical and logical security of intelligent transportation systems ("**ITS**") at UBH. *See* Ex. 2; *see also*, Marx Dec. ¶ 17(a). This policy designated administrative support for UBH's cybersecurity program, including the appointment of a member of UBH's senior leadership to serve as the security official responsible for the development and implementation of policies and procedures required by recognized cybersecurity frameworks like HIPAA and PCI. *See* Ex. 2 § 3.0. The policy also outlined technical and physical safeguards that UBH implemented to protect PII and PHI including restricting access to UBH's server room(s) and perimeter network closets, limiting access to UBH's private networks through personal mobile devices, and mandating periodic cybersecurity audits consistent with national and international standards. *See id*. The policy included correction mechanisms to ensure protocols were updated as new information became available and enforcement mandates to mitigate noncompliance. *See id*. Similarly, the WISP's other nine policies outlined protocols to safeguard PII and PHI, from governing firewalls and remote access to outlining a cadence of steps required when responding to a cyberattack. *See e.g.,*17(a)-(j).

UBH followed these policies and protocols as of the date of the Incident. *See* Marx Dec. ¶¶ 17-38. For example, as of that date, Marx had been serving as the Security Officer under the IST Security Policy. *Id.* ¶ 18. In that capacity, he oversaw the implementation of the WISP,

apprised the organization's executive team on UBH's cybersecurity efforts, and ensured compliance with the protocols adopted to protect PII and PHI. *See id.* ¶ 19. And as required by the ITS Security Policy, UBH engaged an outside consultant to audit its compliance with HIPAA annually and trained healthcare providers and supporting staff on cybersecurity. *See id.* ¶¶ 21-23; Ex. 2 § 3.0 (requiring periodic HIPAA audits). As Hartley summarized, these are all the steps that an organization like UBH can take to protect PHI and mitigate potential unauthorized access to PHI. Hatley Dec. ¶¶ 20-21. In sum, UBH is entitled to an affirmative defense under CADA because as of the date of the Incident, UBH had adopted a WISP that was designed to protect PHI within the meaning of subsection 702(4)(a) and was reasonably complying with the same.

B. UBH's WISP Complied With At Least Three Of The Alternative Frameworks Recognized Under Utah Code Ann. § 78B-4-702(4)(b).

Another requirement under Subsection 702(4) of CADA is that the WISP meet at least one of several *alternative* information security frameworks, three of which UBH invokes here because the potentially exposed information includes PHI. *See id.* § 78B-4-702(4)(b).[14] Specifically, UBH's WISP qualifies under CADA because it (1) "reasonably complied" with the security requirement as described in HIPAA, 45 C.F.R Part 164, Subpart C; (2) "reasonably conform[ed]" to the then existing versions of NIST Special Publications 800-53 and 800-53a;

[14] The applicable framework depends on the type of information at issue. *See e.g.,* Utah Code Ann. § 78B-4-703(1)(a), (b)(iii). For example, CADA provides that where the information exposed by the breach "is regulated by the federal government or state government," the affirmative defense applies if the victim's WISP "reasonably complies with the requirements of the regulation." *Id.* § 78B-4-703(1)(b)(iii). If the data includes payment card information, for example, then the WISP may qualify if it complied with the version of the PCI data security standard effective as of the date of the breach. *See id.* § 78B-4-703(1)(b)(iv). Here, the data that was potentially exposed included PHI, and thus HIPAA is an appropriate framework pursuant to § 78B-4-703(1)(b)(iii)(A).

and (3) consisted of a tailored program under Subsection 703(2) of CADA (a "**Section 703(2) Framework**"). *See id.* §§ 78B-4-703(1)(b)(i), (ii)(A)-(B), (iii)(A). Any one of which, on its own, would satisfy this CADA requirement.

First, UBH was in compliance with the information security framework found in HIPAA's Subpart C regulation. *See* 45 C.F.R. Part 164, Subpart C; *see also*, Utah Code Ann. § 78B-4-703(1)(b)(i). In a nutshell, Subpart C outlines administrative, physical and technical information security standards designed to protect PHI before, during and after a security incident. *See id.* As of the date of the Incident, UBH's WISP complied with Subpart C's framework as detailed in the annual HIPAA Security Risk Analyses conducted by Intraprise Health, an independent outside vendor specializing in data security. *See e.g.*, Ex. 12, 2021 UBH HIPAA Security Risk Analysis at 5-35; *see also*, Marx Dec. ¶¶ 22-23; Hartley Dec. ¶¶ 20-21.[15] Intraprise attested that UBH complied with the requirements of Subpart C before and after the Incident. *See* Exs. 12-14; *see also*, Marx Dec. ¶¶ 21-25.

Second, UBH's WISP reasonably conformed to NIST Special Publication 800-53 and 800-53a. *See* Utah Code Ann. § 78B-4-703(1)(b)(ii)(B). Like HIPAA's Subpart C, NIST 800-53 and 800-53a provides a catalog of security and privacy controls to protect information from a series of threats and risks, including hostile attacks. *See* NIST SP 800-53 Rev. 5 (2020). As with

[15] To illustrate, Subpart C requires that a covered organization "[i]mplement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." 45 C.F.R. § 164.308(a)(1)(ii)(D). According to the 2021 Security Risk Analysis, UBH complied with this requirement by, among other things, adopting and enforcing its ITS Employee Account Policy and ITS Security Policy, *see* Exs. 5 and 2, respectively, instituting a HIPAA Advisory Committee that was headed by UBH's Security Officer, and holding monthly HIPAA Advisory Committee meetings to discuss security audits and system security. *See* Ex. 12, 2021 UBH HIPAA Risk Analysis at 9.

HIPAA's Subpart C, Intraprise attested that UBH was in compliance with the requirements of NIST 800-53. *See e.g.*, Ex. 12, 2021 UBH Security Risk Analysis at 5-35;[16] *see also* Ex. 14, Marx Dec. ¶¶ 22, 24-25.

Third, as of the date of the Incident, UBH's WISP was a "reasonable security program" under § 78B-4-703(2). Under Subsection 703(2),

> A written cybersecurity program is a reasonable security program . . . if:
>
> (a) the person coordinates, or designates an employee of the person to coordinate, a program that provides the administrative, technical, and physical safeguards described in Subsections 78B-4-702(4)(a) and (c);
>
> (b) the program under Subsection (2)(a) has practices and procedures to detect, prevent, and respond to a breach of system security;
>
> (c) the person, or an employee of the person, trains, and manages employees in the practices and procedures under Subsection (2)(b);
>
> (d) the person, or an employee of the person, conducts risk assessments to test and monitor the practice and procedures under Subsection (2)(b), including risk assessments on:
>
> (i) the network and software design for the person;
>
> (ii) information processing, transmission, and storage of personal information; and
>
> (iii) the storage and disposal of personal information; and

[16] In the Assessments, the NIST 800-53 standards and controls are denominated by the initials "AC", "AU", "AT," "CA," "CM" and so on. *See e.g.* Ex. 12, 2021 UBH HIPAA Risk Analysis at 5-35. Each abbreviation identifies the NIST 800-53 control that Intraprise tested. For example, Intraprise attested that as of 2021, UBH's WISP complied with NIST 800-53's IR-1 through IR-8 standards, which address incident response protocols. *See* Ex. 12, 2021 UBH HIPAA Risk Analysis at 19; *see also*, NIST SP 800-53 Rev. 5 (2020).

> (e) the person adjusts the practices and procedures under Subsection (2)(b) in light of changes or new circumstances needed to protect the security, confidentiality, and integrity of personal information.

Utah Code Ann. § 78B-4-703(2).

UBH's WISP meets all these requirements. It designates a Security Officer – at all relevant times here, Marx – to coordinate the program, which provides administrative, technical, and physical safeguards for the PII and PHI. *See e.g.*, Ex. 2, ITS Security Policy; Marx Dec. ¶ 18. UBH's WISP included practices and procedures to detect, prevent and respond to a security breach. *See e.g.*, Ex. 9, ITS Incident Response Policy 9.0; Marx Dec. ¶ 17(j). The WISP also prescribed for periodic training and supervision regarding information security. *See e.g.*, Ex. 2, ITS Security Policy. And the WISP required annual risk assessments like those conducted by Intraprise addressing risks to UBH's network, software, information processing, transmission, storage, and disposal. *See e.g.*, Exs. 12-13, sample HIPAA One Risk Assessments. Lastly, consistent with the WISP, UBH adjusted its practices and procedures in light the results of the assessments, or changed circumstances like the emergence of new threats. *See* Marx Dec. ¶¶ 26-28. Thus, UBH's WISP meets the elements of § 78B-4-702(4) because it is a "reasonable security program" under § 703(2), in addition to meeting the requirements of the HIPAA Subpart C and NIST 800-53 and 800-53a frameworks.

C. UBH's WISP Complied With Subsection 78b-4-702(4)(C)'S Proportionality Requirement As Of The Date Of The Incident.

The final requirement under CADA is that the WISP must be "of an appropriate scale and scope in light of the following factors:"

> (i) the size and complexity of the person;
>
> (ii) the nature and scope of the activities of the person;

> (iii) the sensitivity of the information to be protected;
>
> (iv) the cost and availability of tools to improve information security and reduce vulnerability; and,
>
> (v) the resources available to the person.

Utah Code Ann. § 78B-4-702(4)(c).

Here, UBH's WISP met all of these requirements as of the date of the Incident. *See* Marx Dec. ¶¶ 17-38. Plaintiffs correctly allege that as a hospital providing healthcare services to rural communities in Utah, UBH held fairly sensitive information, including PHI. *See* Marx. Dec. ¶¶ 4-15. But the information security framework most commonly followed and appropriate for the safety and security of PHI is HIPAA's Subpart C. *See* Hartley Dec. ¶¶ 15-21. And here, Intraprise's certifications and analyses show that in the years preceding the Incident, UBH complied with Subpart C and other information security frameworks like NIST 800-53. *See e.g.*, Exs. 12-14. Intraprise's certifications are corroborated by Marx's testimony that prior to and after the Incident, UBH adopted several risk mitigation protocols and processes, including standardizing operating systems for workstations, conducting monthly cybersecurity training for the information technology staff and quarterly anti-phishing testing and training for all staff, and deploying new technologies like network segmentation and monitoring software was they became available. *See* Marx Dec. ¶ 28. Thus, as Hartley concludes, UBH's WISP was of an appropriate scale and scope given UBH's operations, size and resources. *See* Hartley Dec. ¶¶ 20-21.

In sum, UBH is entitled to summary judgment because it is not genuinely disputed that its WISP complied with the requirements of Utah Code Ann. §§ 78B-4-702 and 703, and all of

Plaintiffs' causes of action purport to seek redress for UBH's alleged failure to prevent, respond to, or provide notice of the Incident.

V. IN THE ALTERNATIVE, PLAINTIFFS' COMPLAINT FAILS TO STATE A CLAIM UPON WHICH RELIEF CAN BE GRANTED.

In the alternative, Plaintiffs' Second, Fourth, Fifth, and Seventh causes of action fail to state a claim upon which relief can be granted under Rule 12(b)(6). Defendant addresses each in turn.

A. Plaintiffs' Second Claim, Negligence Per Se, Fails Because The FTCA And HIPAA Do Not Create A Statutory Duty.

In addition to general negligence, Plaintiffs also allege negligence per se based on the FTCA and HIPAA. Compl. ¶¶ 224-225.

In Utah, negligence per se is "conduct, whether of action or omission, which may be declared and treated as negligence without any argument or proof as to the particular surrounding circumstance," and "usually results from the violation of a statute." *Mitchell v. Wells Fargo Bank*, 355 F. Supp. 3d 1136, 1157 (D. Utah 2018). However, "before violation of a legislative standard will be held to be negligence per se . . . the legislative standard must first be adopted by the court as defining the standard of conduct of a reasonable person." *Id.* (internal quotation marks omitted). Whether a statute can form the basis of a negligence per se claim is "closely related to the question of whether a private cause of action exists under a statute." *Cohen v. Ne. Radiology, P.C.*, 2021 U.S. Dist. LEXIS 16497, at *18-19 (S.D.N.Y. Jan. 28, 2021).

Here, Plaintiffs allege UBH breached its duties under both Section 5 of the FTCA and HIPAA. Compl. ¶ 227. But Plaintiffs do not establish that Utah adopted the FTCA or HIPAA as creating a duty that can form the basis of a negligence per se claim. Further, neither the FTCA

nor HIPAA permit a private cause of action. *Am. Airlines v. Christensen*, 967 F.2d 410, 414 (10th Cir. 1992) (FTCA); *Freier v. Colorado*, 804 F. App'x 890, 891 (10th Cir. 2020) (HIPAA). Plaintiffs thus appear to ask this Federal Court to hold, for the first time, that Utah law permits a cause of action based on these two federal statutes that do not provide any private cause of action. Further, other courts have dismissed claims of negligence per se claims on the grounds that neither the FTCA nor HIPAA can sustain a negligence per se claim. *See Cohen*, 2021 U.S. Dist. LEXIS 16497, at *19-20.

Plaintiffs do not allege a violation of any statute that under Utah law can serve the basis of a negligence per se claim, and therefore this claim fails to state a claim and must be dismissed.

B. Plaintiff's Fourth Claim, Unjust Enrichment, Fails Because Plaintiffs Have Not And Cannot Plead That UBH Retained An Improper Benefit Under The Circumstances.

To assert a claim of unjust enrichment, Plaintiffs must establish "(1) there was a benefit conferred on one person by another; (2) the conferee must appreciate or have knowledge of the benefit; and (3) the acceptance or retention by the conferee of the benefit under such circumstances as to make it inequitable for the conferee to retain the benefit without payment of its value." *Hark'n Techs., Inc. v. Orange Whip Fitness X, LLC*, No. 1:21-cv-00054, 2022 U.S. Dist. LEXIS 147702, at *34-35 (D. Utah Aug. 16, 2022). Plaintiffs base their claim on the allegation that they conferred a benefit on UBH by turning over their private information and "paying for healthcare services that should have included cybersecurity protection," but that Plaintiffs did not receive such protection. Compl. ¶ 262. Thus, Plaintiffs allege UBH retained a benefit of "the amounts of payment received from or on behalf of Plaintiffs and Class Members

that should have been used for adequate cybersecurity practices that it failed to provide." *Id.* ¶ 265.

This conclusory allegation is insufficient to establish a prima facie claim of unjust enrichment and the Complaint is otherwise devoid of any factual allegations to establish Plaintiffs' claim. Plaintiffs appear to rely solely on the fact that there was a data incident as proof that UBH did not use the funds for data security purposes, UBH did not provide Plaintiffs with adequate data security, and that UBH's data security was inadequate such that Plaintiffs were not receiving the benefit of the services for which they allegedly paid. But the existence of a data incident does not establish UBH did not pay for data security, failed to provide data security, or that the data security was inadequate. *See Griffey v. Magellan Health Inc*., 562 F. Supp. 3d 34, 50 (D. Ariz. 2021) ("[T]he existence of an adequate data security infrastructure and two data breaches in the same year are not mutually exclusive.") Therefore, as in *Griffey*, Plaintiffs here fail to allege that there was any unjust enrichment conferred on UBH. *See id.* at 50 ("Without [p]laintiffs properly alleging that [defendant's] systems were inadequate, there is no way to establish" a claim for unjust enrichment on the pleadings.).

Plaintiffs fail to allege any facts that they conferred an unjust enrichment on UBH, and therefore their unjust enrichment claim fails.

C. Plaintiffs' Fifth Claim, Breach Of Confidence, Fails Because It Is Not Recognized Under Applicable Law.

Plaintiffs do not provide any authority to support their claim that Utah recognizes a breach of confidence cause of action. And a search of reported cases reveals that Utah does not. *See Raiser v. Church of Jesus Christ of Latter-Day Saints*, No. 2:04-cv-896, 2006 U.S. Dist. LEXIS 7484, at *27 (D. Utah Feb. 7, 2006) (noting it is "questionable" whether such a cause of

action exists under Utah law). Even if Utah did recognize a breach of confidence claim, Plaintiffs' Complaint fails to adequately plead a prima facie case. A breach of confidence "involves the unconsented, unprivileged disclosure to a third party of nonpublic information that the defendant has learned within a confidential relationship." *Farmer v. Humana, Inc.*, 582 F. Supp. 3d 1176, 1189 (M.D. Fla. 2022).

Plaintiffs base their claim on UBH's alleged mismanagement and mishandling of Plaintiffs' private information and UBH's security policies. *See* Compl. ¶ 278. These allegations fail to state a prima facie case because a breach of confidence claim "requires a disclosure." *Farmer*, 582 F. Supp. 3d at 1189 (internal quotation marks omitted). A disclosure is "the act or process of making known something that was previously unknown." *Id.* (internal quotation marks omitted). To survive a motion to dismiss, the plaintiff must allege the defendant "affirmatively shared [ ] information or performed some act that made [the plaintiff's] information known." *Id.* (internal quotation marks omitted). Because there must be an affirmative act by the defendant, a breach of confidence cannot be based on allegations that "a defendant's inadequate security facilitated the theft of information by third-parties." *Id.* (internal quotation marks omitted). Where there are no allegations that UBH disclosed Plaintiffs' information to a third-party, as opposed to a third-party disclosing Plaintiffs' information, a claim for breach of confidence fails as a matter of law.

D. Plaintiffs' Seventh Claim, Invasion of Privacy, Fails Because Plaintiffs Have Not Met The Public Disclosure Element.

An invasion of privacy claim has evolved into four separate torts. *Stien v. Marriott Ownership Resorts*, 944 P.2d 374, 377-78 (Utah Ct. App. 1997); *see also Shattuck-Owen v. Snowbird Corp.,* 2000 UT 94, ¶ 11, 16 P.3d 555, 558 (noting the court adopted the standard set

forth in *Stein*). In the Complaint, Plaintiffs only allege one of the four torts—public disclosure of embarrassing private facts about plaintiff. *See* Compl. ¶ 293 (citing *Shattuck-Owen v. Snowbird Corp.*, 2000 UT 94, 16 P.3d 555 (2000) and the elements of public disclosure of private facts).

To prevail on this claim, Plaintiffs must establish the following three elements "(1) the disclosure of the private facts must be a public disclosure and not a private one; (2) the facts disclosed to the public must be private facts, and not public ones; [and] (3) the matter made public must be one that would be highly offensive and objectionable to a reasonable person of ordinary sensibilities." *Shattuck-Owen*, 2000 UT 94, ¶ 11, 16 P.3d 555.

Public disclosure of private facts requires that the private facts are "made public, by communicating [them] to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." *Id.* ¶ 12 (internal quotation marks omitted). First, Plaintiffs do not allege that UBH communicated their private facts to the public at large. *Cf. Purvis v. Healthcare*, 563 F. Supp. 3d 1360, 1377 (N.D. Ga. 2021) (dismissing an invasion of privacy claim under the intrusion upon seclusion tort where plaintiffs allege a third party carried out a data breach and defendants failed to take sufficient precautions to prevent the breach). Rather, Plaintiffs allege that UBH failed to safeguard their data, but that their private information was "disclosed as a result of the Data Breach," not disclosed by UBH. *See* Compl. ¶¶ 294, 296.

Second, Plaintiffs do not allege their private facts are now substantially certain to become "public knowledge." *Shattuck-Owen*, 2000 UT 94, ¶ 12. Instead, Plaintiffs allege their private information was "accessed and/or stole[n]" by third parties. Compl. ¶¶ 34-35. Having private information accessed and/or stolen by third parties, nowhere near rises to the level of becoming

public knowledge. Where Plaintiffs have not alleged UBH disclosed their information or that their private information is now public knowledge or even substantially certain to become public knowledge, Plaintiffs' claim for invasion of privacy fails.

CONCLUSION

For the foregoing reasons, the Complaint is subject to dismissal for lack of subject matter jurisdiction under Rule 12(b)(1). Separately, all of Plaintiffs' causes of action should be dismissed, with prejudice, because Utah's Cybersecurity Affirmative Defense Act bars all claims related to a cyber incident where, as here, a defendant like UBH fell victim to a data breach despite adopting a qualified written security program. In the alternative, the Second, Fourth, Fifth, and Seventh causes of action fail to state a claim upon which relief can be granted under Rule 12(b)(6).

DATED this 16th day of October, 2023.

HOLLAND & HART LLP

/s/ Blaine J. Benard
Blaine J. Benard
Brent E. Johnson
Engels J. Tejeda
Emily T. Howe
Attorneys for Defendant

30716849_v1